WHAT IS CLAIMED IS:

1. A method for modeling a behavior of normal users in a network in response to an application of a first filtering technique, comprising:

receiving a group of packets from a first user subsequent to the application of the first filtering technique; and

creating at least one model reflecting a behavior of the first user based on the group of packets.

2. The method of claim 1 wherein the at least one model includes Hidden Markov Models.

3. The method of claim 1 further comprising:

associating at least one feature with each packet in the group of packets.

4. The method of claim 3 wherein the at least one feature includes at least one of packet types, characteristics of packet headers, time between similar packets, and characteristics of packet loads.

5. The method of claim 3 further comprising:

associating at least one annotation with the at least one feature, the at least one annotation including an annotation identifying the first filtering technique.

6. The method of claim 5 further comprising:

storing the at least one feature and associated at least one annotation.

7. The method of claim 5 further comprising:

verifying an accuracy of the at least one model using the stored at least one feature and associated at least one annotation.

8. The method of claim 3 wherein the creating includes:

creating at least one model based on the features associated with the received packets.

9. The method of claim 1 further comprising:

applying a different filtering technique;

receiving additional packets from the first user after applying the different filtering technique; and

creating additional models reflecting the behavior of the first user based on the additional packets.

10. The method of claim 1 wherein the receiving includes:

receiving a stream of packets from a plurality of users,

identifying the packets in the stream to obtain identified first user packets, and

grouping said identified first user packets.

11. A system for modeling normal user behavior in a network, comprising:

a memory configured to store instructions; and

a processor configured to execute the instructions to:

filter packets in the network using a first filtering technique,

receive a group of packets from a first user after the filtering, and

create at least one model reflecting a behavior of the first user based on the group of packets.

12. The system of claim 11 wherein the at least one model includes Hidden Markov Models.

13. The system of claim 11 wherein the processor is further configured to:

associate at least one feature with each packet in the group.

14. The system of claim 13 wherein the features include at least one of packet types, characteristics of packet headers, time between similar packets, and characteristics of packet loads.

15. The system of claim 13 wherein the processor is further configured to:

associate at least one annotation with the at least one feature, the at least one annotation including an annotation identifying the first filtering technique.

16. The system of claim 15 wherein the processor is further configured to:

store the at least one feature and associated at least one annotation in the memory.

17. The system of claim 15 wherein the processor is further configured to:

verify an accuracy of the at least one model using the stored at least one feature and associated at least one annotation.

18. The system of claim 13 wherein, when creating the at least one model, the processor is configured to:

create the models based on the features associated with the group of packets.

19. The system of claim 11 wherein the processor is further configured to:

apply, after creating the at last one model, a second filtering technique,

receive a subsequent group of packets from the first user after applying the second filtering technique, and

create additional models reflecting the behavior of the first user in response to the second filtering technique.

20. The system of claim 11 wherein, when receiving the group of packets, the processor is configured to:

receive a stream of packets from a plurality of users,

identify the packets in the stream, and

group packets from the first user.

21. A computer-readable medium containing instructions for controlling at least one processor to perform a method for modeling a behavior of users in a network in response to having at last one packet dropped, comprising:

receiving, subsequent to the at least one packet being dropped, a number of packets from a first user; and

creating at least one model reflecting a behavior of the first user based on the received packets.

22. The computer-readable medium of claim 21 wherein the at least one model includes Hidden Markov Models.

23. The computer-readable medium of claim 21 wherein the method further comprises:

associating at least one feature with each packet from the first user,

wherein the at least one feature includes at least one of packet types, characteristics of packet headers, time between similar packets, and characteristics of packet loads.

24. The computer-readable medium of claim 21 wherein the receiving includes:

receiving a stream of packets from a plurality of users, and

grouping packets associated with the first user.

25. A method for protecting against network attacks that includes detecting an attack and applying a filtering technique, comprising:

receiving, subsequent to the filtering technique being applied, a stream of packets;

partitioning the packets into groups, each group corresponding to a plurality of packets;

classifying each group of packets as a normal group or an attack group using at least one model, each model reflecting a normal response to an application of the filtering technique; and

allowing the normal groups to pass on toward their destination.

26. The method of claim 25 further comprising:

identifying each packet in the stream; and

associating at least one feature with each packet.

27. The method of claim 26 wherein the features include at least one of at least one type of packets, characteristics of packet headers, time between similar packets, and characteristics of packet loads.

28. The method of claim 26 wherein the classifying includes:

identifying, for each group of packets, the at least one model from a plurality of previously created models,

comparing the features associated with a group of packets with features of each of the at least one identified model,

generating a closeness score for each of the at least one identified model based on the comparing,

determining whether the closeness score for each of the at least one identified model equals or exceeds a threshold, and

identifying the group of packets as a normal group when the closeness score of at least one of the identified models equals or exceeds the threshold.

29. The method of claim 25 further comprising:

applying the filtering technique to the attack groups.

30. The method of claim 25 wherein the at least one model includes Hidden Markov Models.

31. The method of claim 25 wherein the at least one model relates to the filtering technique.

32. A system for identifying normal traffic during a network attack, comprising:

means for receiving, subsequent to a filtering technique being applied, a stream of packets;

means for partitioning the packets into groups, each group corresponding to a plurality of packets; and

means for classifying each group of packets as a normal group or an attack group using at least one model, each model reflecting a normal response to an application of the filtering technique.

33. A system for identifying normal traffic during a network attack, comprising:

a memory configured to store a plurality of models, each model reflecting a normal response to an application of a filtering technique; and

a processor connected to the memory and configured to:

receive a stream of packets subsequent to a first filtering technique being applied,

partition the stream into strands, each strand corresponding to a plurality of packets, and

classify each strand as at least one of a normal strand and an attack strand using at least one of the plurality of models.

34. The system of claim 33 wherein processor is further configured to:

allow traffic corresponding to normal strands to pass on toward their destination.

35. The system of claim 34 wherein the processor is further configured to:

filter traffic corresponding to attack strands using the first filtering technique.

36. The system of claim 34 wherein, when partitioning, the processor is configured to:

group packets in the stream based on a source of the packets.

37. The system of claim 33 wherein the processor is further configured to:

associate, prior to partitioning, at least one of a plurality of previously defined features with each packet in the stream.

38. The system of claim 37 wherein, when classifying, the processor is configured to:

identify, for each strand, at least one model from the plurality of models,

compare the features associated with each strand with features of each of the at least one model,

generate, for each strand, a closeness score for each of the at least one models based on the comparing,

determine, for each strand, whether the closeness score for each model equals or exceeds a threshold, and

identify a strand as a normal strand when the closeness score for at least one model equals or exceeds the threshold.

39. The system of claim 38 wherein the at least one identified model includes models associated with the first filtering technique.

40. The system of claim 34 wherein the plurality of models include Hidden Markov Models.

41. A computer-readable medium containing instructions for controlling at least one processor to perform a method for identifying normal traffic during a network attack, comprising:

receiving, subsequent to an application of a first filtering technique, a stream of packets;

grouping packets in the stream based on at least a source of the packets; and

identifying, through the use of Hidden Markov Models (HMMs), each packet group as a normal group or attack group, the HMMs representing normal responses to the application of the first filtering technique.

42. The computer-readable medium of claim 41 further comprising:

associating, prior to grouping, at least one feature with each packet in the stream of packets.

43. The computer-readable medium of claim 42 wherein the identifying includes:

identifying, for each packet group, at least one HMM from a plurality of previously created HMMs,

comparing the features associated with a packet group with features of each of the at least one HMMs,

generating a closeness score for each of the at least one HMMs based on the comparing,

comparing each closeness score to a threshold, and

identifying the packet group as a normal group when at least one of the closeness scores equals or exceeds the threshold.

44. A network comprising:

a first device configured to:

create models to reflect a behavior of normal users in the network in response to an application of at least one filtering technique, and

transmit the models; and

at least one second device configured to:

receive the models from the first device,

use the models to identify normal traffic in the network once an attack has been detected and filtering applied, and

allow identified normal traffic to pass on toward its destination.

45. The network of claim 44 wherein the models include Hidden Markov Models.